TABLA DE CONTENIDO

Tabla de contenido

	Revisó	Aprobó
Cargo	Coordinador de Riesgos y Cumplimiento	Gerente General
Firma		

CONTROL DE CAMBIOS

VERSION	FECHA DE APROBACION	NUMERAL O CAPITULO ACTUALIZADO	DESCRIPCION DEL CAMBIO REALIZADO
1			Primera versión

1. OBJETIVOS

Definir las políticas y procedimientos de Seguridad de la Información y Ciberseguridad

2. ALCANCE

Termovalle SAS ESP

3. DEFINICIONES

Activos de software: software de aplicación, software del sistema, herramientas de desarrollo y otros equipos.

Activos físicos: equipos de computación, equipos de comunicaciones, medios removibles y otros equipos.

Alertas: Es un evento generado por alguna violación a las políticas de seguridad de la información, el cual es reportado en el momento en que ocurren a la persona que debe darle atención.

Autenticación: Es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse.

Ciberseguridad: Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.

Ciclo de vida de la información: Cubre todos los eventos relacionados desde la creación de la información, durante su uso autorizado y hasta su apropiada disposición o destrucción.

Confiabilidad: Propiedad de la información de ser consistente en su comportamiento.

Confidencialidad: Propiedad de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Controles: conjunto de acciones, normas, documentos, procedimientos y medidas técnicas adoptadas para propender porque cada amenaza, identificada y valorada con un cierto nivel de riesgo, sea minimizada.
Disponibilidad: Propiedad de ser accesible y utilizable por pedido de una entidad autorizada.

Efectividad: La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.

Eficiencia: La información se usa en actividades planificadas y los resultados son planificados.

Incidente de seguridad de la información: Uno o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones y amenazar la seguridad de la información. Los incidentes de seguridad se presentan por el mal uso de los recursos informáticos o por eventos que atenten contra la confidencialidad, integridad y disponibilidad de la información.

Información: Elemento que genera, procesa y/o resguarda información necesaria para la operación y el cumplimiento de los objetivos de Termovalle. Algunos ejemplos son las bases de datos y archivos de datos, contactos y acuerdos, documentación de los sistemas, información sobre investigación, manuales de usuario, material de formación, procedimientos operativos o de soporte, planes para

la continuidad del negocio, acuerdos de recuperación, registros de auditoría e información archivada.

Integridad: Propiedad de la información de ser exacta y completa a través de su ciclo de vida.

Modelo de Seguridad de la Información: Requisitos de seguridad de un sistema de información, servicio o de sus elementos. Son todas las políticas, normas, estándares, procesos, procedimientos, guías y herramientas de hardware y software necesarios para prevenir, detectar y reaccionar frente a algún evento que atente contra la seguridad de la información. Es una expresión formal, matemática, de la política de general de seguridad de la información. Es en últimas la materialización de la política en mecanismos de seguridad.

Monitoreo: Es una revisión permanente para determinar el estado de un sistema, un proceso o una actividad

No repudio: Capacidad de probar la ocurrencia de un evento o acción reclamada y sus entidades originadoras. La propiedad de no repudiación de un sistema de seguridad de redes de cómputo se basa en el uso de firmas digitales.

Norma: Conjunto de reglas requeridas para implantar las políticas. Las normas hacen mención específica de tecnologías, metodologías, procedimientos de aplicación y otros factores involucrados y son de obligatorio cumplimiento.
Otra información: personas y sus calificaciones, habilidades y experiencia; Intangibles tales como reputación e imagen de la organización.

Perímetros o áreas seguras: Un área o agrupación dentro de la cual un conjunto definido de políticas de seguridad y medidas se aplica, para lograr un nivel específico de seguridad. Las áreas o zonas son utilizadas para agrupar entidades con requisitos de seguridad y niveles de riesgo similares y de esta forma asegurar que cada zona se separa adecuadamente de las otras.

Privacidad: Es el derecho a mantener el secreto sobre los datos inherentes a la organización y comunicaciones y a utilizarla exclusivamente para los propósitos con que fue obtenida.

Procedimientos: Pasos operacionales específicos que los individuos deben tomar para lograr las metas definidas en las políticas.

Propietario activo de información: Un individuo o unidad organizacional que tiene responsabilidad por clasificar y tomar decisiones de control con respecto al uso de su información.

Riesgo de seguridad de la información: El riesgo de seguridad de la información

está asociado con el potencial de ocurrencia de un evento de seguridad de la información que cause daño a la organización.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Seguridad física: La protección de los equipos de procesamiento de la información de daños físicos, destrucción o robo; Protege las facilidades asignadas para el procesamiento de la información de daño, destrucción o ingreso desautorizados; y al personal de las situaciones potencialmente dañinas.

Servicios: servicios de computación y comunicaciones, servicios generales como por ejemplo iluminación, calefacción, energía y aire acondicionado.

Sistema de Gestión de Seguridad de Información (SGSI): Es un conjunto de políticas, procesos, procedimientos y Controles que interactúan entre sí, propendiendo por que los riesgos relacionados con los Activos de Información sean identificados, conocidos, asumidos, tratados, minimizados y monitoreados por el grupo Termovalle, de una forma estructurada, eficiente, documentada y adaptada a los cambios que se produzcan en los riesgos, el entorno y la tecnología.

Terceros: Son los proveedores, clientes y contratistas.

4. POLÍTÍCA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Termovalle, debe proteger los activos de información y ciberactivos críticos, que soportan los procesos de la empresa, garantizando la confidencialidad, integridad y disponibilidad de los mismos, adicionalmente, cumplirá los requisitos legales y contractuales que en materia de seguridad de la información o cibernética le apliquen y mejorará continuamente sus habilidades para mitigar los riesgos, en concordancia con los objetivos estratégicos de la organización.

Todos los empleados, deben conocer sus responsabilidades respecto a la seguridad de la información y deben cumplir las políticas y procedimientos que se emitan al respecto, propendiendo siempre por disminuir el nivel de exposición a los riesgos.

4.1 REVISIÓN Y APROBACIÓN DE LAS POLÍTICAS

El Coordinador de Riesgos y Cumplimiento, es el responsable de la redacción de las políticas, las cuales serán socializadas y aprobadas en el Comité de Riesgos y/o el Gerente General. Así mismo, anualmente, se hará una revisión de las Políticas y Procedimientos de Seguridad de la Información y su resultado será presentado al Comité de Riesgos. Esta revisión hará parte de las actividades del Plan de Trabajo Anual del Coordinador de Riesgos y Cumplimiento. Así mismo, en caso de ser

necesario, se realizará la revisión de la política y de los procedimientos de seguridad de la información en caso de que se presenten cambios significativos en la estructura de Termovalle en cuanto a sus procesos y plataforma tecnológica.

El Coordinador de Riesgos y Cumplimiento, en nombre del Gerente General, es el responsable de formalizar y divulgar las políticas de Seguridad de la Información y Ciberseguridad.

4.2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.2.1 Roles y responsabilidades de la seguridad de la información

4.2.1.1 Comité de Riesgos:

El Comité de Riesgos de la Organización, es el órgano responsable de:

- Aprobar las políticas de Seguridad de la Información y Ciberseguridad y hacer seguimiento al cumplimiento de las mismas.
- Promover el cumplimiento de las políticas a través de toda la organización.

4.2.1.2 Coordinador de Riesgos y Cumplimiento

Como encargado de la seguridad de la información:

- Aplicar conocimientos, habilidades, herramientas y técnicas que permitan diseñar un programa de seguridad de la información y ciberseguridad, que cumpla con las normas requeridas y con las necesidades de la organización y presentarlo para su aprobación al Comité de Riesgos.
- Identificar, analizar, evaluar y tratar los riesgos cibernéticos y de seguridad de la información de la organización.
- Identificar brechas de control respecto a normatividades, buenas prácticas o políticas internas.
- Planear, implementar y hacer seguimiento a las tareas, fechas y planes de trabajo relacionados con el programa.
- Definir los roles y responsabilidades en materia de seguridad de la información, para los cargos de la organización.
- Conocer el estado de cumplimiento de las políticas definidas e informar las desviaciones o incumplimientos al Comité de Riesgos.
- Velar por el mantenimiento de la documentación relacionada con seguridad de la información y ciberseguridad.
- Administrar la base de datos de Incidentes y eventos de seguridad de la información y ciberseguridad, establecer planes de acción y mitigación.

4.2.1.3 Tecnología, seguridad física, gestión documental y mantenimiento:

Las áreas de: Mantenimiento, Gestión Tecnológica (Gerencia y Dirección Financiera y Administrativa, a través del proveedor de tecnología de la organización), Gestión documental y Seguridad Física, son parte del programa de seguridad de la información, por lo tanto sus líderes, son responsables de:

- Aplicar conocimientos, habilidades, herramientas y técnicas que permitan diseñar un programa de seguridad de la información y ciberseguridad, que cumpla con las normas requeridas y con las necesidades de la organización. Esto debe ser informado al Coordinador de Riesgos y Cumplimiento.
- Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar por parte del Coordinador de Riesgos y Cumplimiento.
- Gestionar los riesgos de seguridad de la información y ciberseguridad de la entidad.
- Participar junto con el Coordinador de Riesgos y Cumplimiento, en el diseño de las políticas, normas y procedimientos de seguridad de la información y ciberseguridad.
- Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de la información y velar por su cumplimiento, actuando bajo el marco de actuación ética establecido.
- Proponer la implementación de herramientas, metodologías o controles para la mitigación de riesgos cibernéticos.
- Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad.
- Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias.
- Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.
- Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
- Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.

4.2.1.4 Líderes de proceso

Los líderes de proceso son los responsables de la administración, operación y gestión de la seguridad de la información en su proceso, garantizando la segregación de funciones, para minimizar las posibilidades de modificación no autorizadas o el uso indebido de los activos de información.

4.2.1.5 Todos los empleados

Los empleados, contratistas y otros terceros, están obligados a cumplir con las políticas, normas y procedimientos que se establezcan respecto a la seguridad de la información y ciberseguridad

4.2.2 Conctacto con autoridades y grupos de interés.

Dentro de la gestión de seguridad de la información, se podrá mantener contacto con las autoridades pertinentes así como con los grupos de interés que sean necesarios, de acuerdo a la normatividad que lo reglamente. Así mimo, queda abierta la posibilidad de realizar los reportes a las autoridades, de aquellos incidentes de Ciberseguridad que así lo ameriten.

4.2.3 Seguridad de la información en la gestión de proyectos

Los proyectos que ejecute Termovalle, deberán gestionar la seguridad de la información como los demás procesos de la organización. Así mismo, deberán evaluar los impactos que pueda tener la seguridad de la información por la implementación de los cambios que genere el proyecto.

4.2.4 Dispositivos móviles y teletrabajo

Los dispositivos móviles que hagan uso de información de Termovalle o que se conecten a su red se deben acoger a las políticas de seguridad de la información definidas en el presente manual.

- Al conectar un dispositivo a la red de Termovalle, el propietario del dispositivo acepta las políticas definidas en el presente manual y así mismo, las disposiciones que estas determinen.
- La Dirección Administrativa y Financiera, junto con el proveedor de los servicios de tecnología, debe disponer de un mecanismo de conexión seguro que garantice que las conexiones de teletrabajo autorizadas se realizan de forma segura y se protegen los activos de información en uso

4.3 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

4.3.1 Normas respecto a la vinculación

1. El área de Gestión Humana, debe garantizar el cumplimiento del proceso de selección de todos los candidatos a un cargo, incluyendo el cumplimiento de la política de vinculación del SAGRLAFT.

2. Todos los empleados que sean vinculados a la organización, tienen la responsabilidades frente a la Seguridad de la Información, su compromiso de no divulgar información interna o externa o la relacionada con sus funciones a través de ningún canal, sin previa autorización y la aceptación de pruebas y revisiones de seguridad durante la relación laboral, sin que eso conlleve a la violación de sus garantías constitucionales. Esta responsabilidad es asignada por la Dirección de Termovalle y podrá hacer parte del reglamento interno de trabajo.

3. El proveedor de tecnología, debe garantizar que todos los empleados de su organización, que prestan el servicio como contratistas de Termovalle, cumplen con un proceso de selección adecuado, que incluye revisiones de seguridad.

4. El proveedor de tecnología, debe garantizar que todos los empleados de su organización, cuentan con acuerdos contractuales que incluyen sus responsabilidades frente a la seguridad de la información con Termovalle.

5. Los terceros que requieran acceder a las instalaciones o a la plataforma tecnológica de la organización, deben firmar un acuerdo de confidencialidad, que indique sus responsabilidades frente a la seguridad de la información y acepte la política de la organización.

4.3.2 Normas durante la ejecución de labores contractuales:

1. Los encargados de Seguridad de la Información, deben implementar un programa de capacitación y sensibilización en seguridad de la información y ciberseguridad, dirigido a todos los empleados y contratistas.

2. Todos los empleados de la organización, deben asistir a los eventos o capacitaciones que se realicen en relación con la seguridad de la información y la ciberseguridad.

3. Todos los empleados, deben actuar de forma ética de acuerdo a los dispuesto en el Código de Ética y conducta / Normas de integridad y deben ser cuidadosos de no divulgar información a personas no autorizadas, en lugares públicos, conversaciones o en otras situaciones.

4. Todos los empleados vinculados con la organización, deben manejar la información a la que tenga acceso y que sea verbal, física o electrónica, de forma íntegra e integral, es decir que se debe adoptar, procesar, entregar o transmitir integralmente y coherentemente, sin modificaciones, ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información.

5. Cuando existan violaciones a las políticas de Ciberseguridad y Seguridad de la Información, se iniciará un proceso disciplinario, en donde participarán las siguientes áreas: Gestión Humana, Legal, Riesgos y Cumplimiento, con el fin de evaluar la falta cometida.

4.3.3 Normas respecto a la terminación o cambio de contrato

1. El área de Gestión Humana debe realizar el procedimiento de desvinculación, otorgamiento de licencias, incapacidades, vacaciones o cambio de labores de los empleados de Termovalle llevando a cabo los procedimientos que se hayan establecido.

2. Los dueños de proceso, debe reportar de manera inmediata al área de Gestión Humana, la desvinculación o cambio de labores de los empleados o del personal provisto por terceras partes, con el fin que se tomen las medidas pertinentes.

4.4 ADMINISTRACIÓN DE ACTIVOS

4.4.1 Responsabilidad por los activos

1. La Coordinación de Riesgos y Cumplimiento, establecerá la metodología para identificar los activos de información (Hardware, software, servicios, información y recursos humanos) y elaborar el inventario y clasificación de los mismos.

2. La Dirección Administrativa y Financiera es la propietaria de los activos de información correspondientes a la plataforma tecnológica, por lo tanto debe asegurar su apropiada administración y operación.

3. La Gerencia de Producción, es la propietaria de los activos de información correspondientes a la operación de la planta de producción, por lo tanto debe asegurar su apropiada administración y operación.

4. Los propietarios de los demás activos de información, son los Gerentes y/o Directores de las áreas, por lo tanto ellos deben garantizar:

    - Que todos los activos de información de su área, sean identificados de acuerdo al procedimiento de activos de información, sean clasificados en función de sus requisitos legales, valor, criticidad y susceptibilidad a divulgación o modificación no autorizada y que estos se encuentren actualizados permanentemente.
    - Que cuando un empleado, contratista o tercero finalice el empleo, acuerdo o contrato, devuelva los activos físicos y de información, entregados durante su vinculación.

- Los empleados deben conocer y cumplir con las políticas y procedimientos de la gestión de activos, mantener actualizado el inventario de activos de información y deben propender por mitigar los riesgos a los que se exponen.

4.4.2 Clasificación de la información

1. El proveedor de tecnología cuenta con mecanismos de protección de los activos administrativos (Firewall, Antivirus etc) de acuerdo a su clasificación. Previa autorización de la Dirección Administrativa y Financiera.

2. La Gerencia de Producción, establecerá e implementará los mecanismos de protección de los ciberactivos críticos.

3. El proveedor de tecnología y la Gerencia de Producción, cuentan con mecanismos de protección de los activos de información y ciberactivos críticos.

4. Toda la información de la organización, debe ser clasificada, aquella que no cuente con clasificación, debe ser tratada como información sensible.

5. El Coordinador de Riesgos y Cumplimiento, junto con los líderes de proceso y Gestión Humana, realizaran evaluación de los cargos, respecto a la clasificación de información a la cual tienen acceso por cargo o función que desempeñan, a los datos que producen o decisiones que toman y a la necesidad del cargo respecto al proceso y otros atributos. Esto con el fin de tratar el riesgo cibernético por pérdida de personal clave.

6. Todos los empleados deben conocer y cumplir con los procedimientos establecidos para la protección de los activos de información, de acuerdo a la clasificación establecida.

7. El etiquetado de los activos corresponde a la clasificación otorgada en el inventario de activos de información y en las tablas de retención, sin embargo si se requiere, estos podrán ser etiquetados físicamente con un rotulo que indique si es activo crítico, mediamente crítico o no crítico y su clasificación respecto a la confidencialidad, integridad y disponibilidad.

4.5 CONTROL DE ACCESO

4.5.1 Normas para el suministro de control de acceso

1. Los Gerentes y/o Directores de las áreas, son los responsables de autorizar la creación, modificación, suspensión o eliminación de usuarios de los empleados a su cargo y deben garantizar que los permisos que autoricen, se limiten estrictamente a las funciones y roles específicos de cada usuario.

2. Los empleados o terceros que cuenten con usuarios que tengan privilegios superiores y que se utilicen para la administración de infraestructura, aplicaciones o sistemas de información, deben garantizar que el acceso a estos, se realice únicamente por personas autorizadas.

3. Se debe disponer de forma permanente con una matriz de roles versus privilegios de acceso donde se identifique claramente, descripción de los roles, los tipos de accesos de los diferentes roles a los sistemas y a la información de la empresa, esto incluye pero no se limita a servidores de archivos, carpetas compartidas, impresoras, scanners, fotocopiadoras, bases de datos, documentos digitalizados, servidores web, aplicaciones, correo electrónico que se pueda visualizar en dispositivos personales, etc.

4. Se debe contar con la trazabilidad de cambios de la matriz de roles vs privilegios, respecto a los derechos de acceso, ajustes o retiros que se realicen sobre cada usuario y esta debe ser revisada cada año, por el dueño del activo con el fin de validar que el personal no tiene privilegios adicionales a los ya autorizados o que no se encuentran activas cuentas de usuarios retirados.

5. El área de Gestión Humana, es responsable de informar oportunamente al proveedor de tecnología, las novedades de personal como: Ingresos y desvinculaciones. Los líderes de área, deben reportar: vacaciones, licencias o incapacidades, con el fin de que se realice la eliminación, o inactivación de los privilegios para acceder a la red, sistemas y aplicaciones y/o cambio de claves del correo electrónico.

6. El proveedor de tecnología y los administradores de las aplicaciones, deben garantizar, que cuando los empleados se desvinculan, estén de vacaciones, con licencias o incapacidades, máximo un (1) día después, se realice la eliminación, o bloqueo de los privilegios para acceder a la red, sistemas y aplicaciones.

7. El proveedor de tecnología, debe implementar métodos de autenticación a las redes inalámbricas, con el fin de evitar el acceso no autorizado.

8. El proveedor de tecnología, debe restringir y controlar el uso de programas utilitarios que tengan la capacidad de anular el sistema y los controles de las aplicaciones.

9. El encargado de la Gestión Documental, debe llevar el control y registro de la información física que se requiera consultar.

4.5.2 Normas para el acceso y gestión con usuario y contraseña

1. Cada empleado, contratista o tercero debe tener un usuario y contraseña para el acceso a redes, aplicaciones o sistemas de información de la organización.

Cuando se trate de terceros, estos solo podrán acceder a un segmento de red diferente a la de los servicios de la organización, excepto si están autorizados por el Gerente del Área.

2. Los empleados, contratistas o terceros a quienes se les haya asignado un usuario y/o contraseña, son responsables de su buen uso, teniendo en cuenta que estas son personales e intransferibles por lo que se prohíbe su divulgación o comunicación a personas no autorizadas.

3. Los empleados, contratistas o terceros a quienes se les haya asignado un usuario y contraseña, son responsables por salvaguardar la información a la cual tienen acceso.

4. El proveedor de tecnología de la organización, debe establecer los parámetros para la configuración de contraseñas que se deben aplicar sobre la plataforma tecnológica (que aplique) y que garanticen un acceso seguro a la red de la organización (Ver parámetros).

5. Los administradores de las aplicaciones de la operación, mantenimiento y planta, deben establecer mecanismos para garantizar que las contraseñas que se utilicen para acceder de forma segura a los activos de información, cumplan con los parámetros mínimos de calidad para que sean un mecanismo de autenticación eficaz y que cuenten con procedimientos para la gestión del cambio de la misma.

6. El Proveedor de Tecnología y los administradores de los sistemas y aplicativos de la organización, deben certificar que no se almacenen, cadenas de conexión, contraseñas u otra información clasificada como sensible en texto claro.

7. Los aplicativos o sistemas de información usados en la operación deben impedir la visualización en pantalla de las contraseñas.

8. Los certificados o las claves deben hacer parte de un procedimiento de custodia de contraseñas que permita el uso de las mismas ante emergencias.

4.5.3 Normas para el acceso a la plataforma de seguridad.

El acceso a las opciones de configuración del Firewall Local está prohibido para el usuario final, a este solo puede acceder el Proveedor de Tecnología.

4.5.4 Normas para el acceso a Internet

1. El envío de información por vía electrónica y el uso de Internet por parte del personal está limitado al desempeño de sus actividades en la empresa.

2. El ingreso a páginas como: Facebook, youtube, Instagram, twitter, entre otras, deben ser autorizadas por el Gerente o Director del área.

3. El firewall, debe contar con una seguridad gestionada

4.5.5 Normas para el acceso a medios removibles

1. Es responsabilidad de los Gerentes o Directores de área aprobar por cada funcionario a su cargo, el uso de medios removibles tales como discos duros removibles, quemadores de CD/DVD o unidades de almacenamiento USB y debe justificar la necesidad del uso del mismo.

2. Los medios removibles que se requieran utilizar en activos críticos de la organización, serán otorgados por la empresa y cumplirán con las revisiones y actualizaciones de antivirus que realice el proveedor de tecnología. Está prohibido utilizar medios removibles personales en dichos activos.

3. El proveedor de tecnología, es el responsable de garantizar que los equipos de los empleados que no tengan permiso para el uso de medios removibles, tengan restringida la conexión.

4.5.6 Normas respecto a los dispositivos móviles

1. Los Gerentes y Directores de área, son los responsables de autorizar la movilización de los computadores portátiles fuera de la organización.

2. De acuerdo a la política de clasificación de activos, está prohibido copiar o descargar información sensible y privada en dispositivos móviles como: Celular, tableta o computador personal o guardar información en la nube.

3. Todos los empleados, deben evitar el uso de los dispositivos móviles en lugares que no ofrezcan condiciones de seguridad adecuadas.

4. Ningún empleado puede deshabilitar las configuraciones de seguridad que establezca el proveedor de tecnología.

4.5.7 Normas para la conexión remota

1. Los Gerentes de área y/o Directores, son los responsables de autorizar a los usuarios que podrán acceder de forma remota a la plataforma tecnológica de la organización, teniendo en cuenta la clasificación de los activos que maneja y los riesgos relacionados.

2. El proveedor de tecnología, debe establecer los métodos y controles para que los usuarios se conecten de forma remota a la red de la organización de una forma segura y controlada.

3. Ningún empleado, debe conectarse a la plataforma tecnológica de la organización, en computadores públicos, desconocidos o desde equipos no seguros.

4. La conexión que se realice a través de acceso remoto desde el exterior de la red LAN hacia los servidores de la organización, debe ser a través de una VPN segura y no se puede realizar en sitios públicos como café internet.

4.6 CRIPTOGRAFIA

En caso de que Termovalle cuente con controles criptográficos, se deberán cumplir con los siguientes aspectos, que serán liderados por el Coordinador de Riesgos y Cumplimiento:

- Desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
- Desarrollar e implementar una política sobre el uso, protección y vida útil de las claves criptográficas durante toda su vida útil.

4.7 SEGURIDAD FÍSICA Y DEL AMBIENTE

1. El proceso de seguridad física, debe identificar todos los puntos de acceso físico a la organización y debe establecer las medidas para controlar el acceso.

2. Deben existir controles de acceso con mecanismos de autenticación a la entrada principal de la sede de la empresa, zona de operación, pre almacenamiento, almacenamiento, custodia documental y de backups; adicionalmente, los lugares donde estén ubicados UPS, centrales telefónicas, rack de comunicaciones, tableros eléctricos, custodia de backups y CCTV, deben tener condiciones ambientales adecuadas.

3. Se debe tener un circuito cerrado de televisión (CCTV) que cubra: la zona de entrada y el interior de área donde se ejecuta la operación; y aquellas zonas en las que se encuentren ubicados los servidores del sistema y los rack de comunicaciones. El tiempo de retención y custodia de los registros del monitoreo, debe ser establecido por el líder del proceso, teniendo en cuenta lo establecido legalmente.

4. Se deben establecer los procesos, herramientas y procedimientos para monitorear el acceso físico.

5. Se debe documentar e implementar los mecanismos procedimentales y técnicos para registrar las entradas en todos los puntos de acceso.

6. Los sistemas de seguridad física, deben contar con un plan de mantenimiento y de pruebas.

7. Las áreas donde se ejecuta la operación de la empresa deben ser cerradas, delimitadas y exclusivas.

8. Las instalaciones deben contar con un plan de respuesta a emergencias, que incluya entre otros, la verificación de que los elementos químicos dispuestos para la extinción de incendios, sean los apropiados para el tipo de material que se encuentra en la zona a proteger.

9. Los empleados deben seguir el procedimiento de control de acceso de Seguridad Física.

4.8 SEGURIDAD DE LAS OPERACIONES

4.8.1 Normas respecto a procedimientos operacionales y responsabilidades.

1. La Gerencia de Producción, es la encargada de la operación en las instalaciones de procesamiento de información, por lo tanto debe asegurar que estas sean correctas y seguras.

2. El proveedor de tecnología, es el responsable de la administración y operación de los sistemas operativos, servicios de red, bases de datos, plataforma de seguridad y tecnológica.

3. Los procedimientos de operación de las instalaciones de procesamiento de información, deben estar documentados y a disposición de los que lo requieran.

4. Se deben establecer procedimientos de monitoreo y seguimiento a la disponibilidad, capacidad y desempeño de los recursos tecnológicos.

5. El proveedor de tecnología y el área de Mantenimiento, deben establecer los procedimientos de control de cambios y gestión de configuraciones para adiciones, modificaciones, reemplazos o retiros de hardware o software de los activos de información y ciber activos críticos, buscando afectar de forma mínima la disponibilidad.

6. Los cambios de las aplicaciones administrativas, deben desarrollarse y probarse en un ambiente diferente al de producción, con el fin de minimizar la indisponibilidad del servicio y deben en lo posible usar datos enmascarados o transformados y no datos reales en estos ambientes. Una vez se finalicen las etapas de desarrollo y pruebas del software se deberá ejecutar un procedimiento de borrado seguro de los datos utilizados. En caso de que la aplicación no permita cumplir esta norma, se debe dejar documentado y realizar los controles necesarios para mitigar el riesgo.

7. Todo soporte técnico que un externo preste sobre los sistemas o computadores asignados a la operación, debe estar supervisado por personal de la empresa o del proveedor de tecnología.

4.8.2 Normas respecto a la protección contra códigos maliciosos

1. El proveedor de Tecnología y el Coordinador de Riesgos y cumplimiento, deben establecer programas de concientización, para proteger la información y las instalaciones de procesamiento contra códigos maliciosos.

2. El proveedor de tecnología, con previa autorización de la Dirección Financiera y Administrativa, debe implementar herramientas para detectar y prevenir códigos maliciosos y debe garantizar su actualización periódica.

3. Todos los equipos de la organización deben estar protegidos con las herramientas establecidas para detectar y prevenir códigos maliciosos y se debe asegurar que ningún usuario pueda realizar cambios sobre las configuraciones de las herramientas definidas. En caso de que en algunos equipos no sea posible cumplir esta norma, se debe dejar documentado y realizar los controles necesarios para mitigar el riesgo.

4. Todos los empleados deben garantizar que los archivos descargados de internet o de un correo electrónico, provienen de una fuente segura.

4.8.3 Normas sobre el control del software operacional

1. El software de todos los sistemas de la organización tanto administrativos como de Producción, debe contar con soporte de proveedores o fabricantes

2. Toda actualización de software, debe realizarse de manera controlada y se deben evaluar los riesgos que pueden generar las actualizaciones del mismo.

3. Los accesos a los proveedores, para la actualización del software, deben ser temporales y estar controlados y monitoreados.

4.8.4 Normas para la gestión de vulnerabilidad técnica

1. Cuando se establezca, se realizarán pruebas de penetración tipo hacking Ético en la infraestructura tecnológica.

2. La Gerencia de Producción y/o el proveedor de tecnología, son los responsables de realizar los planes de acción derivados de las pruebas de penetración.

3. Los empleados, no deben instalar software no autorizado en la plataforma tecnológica de la organización. Todas las solicitudes para la instalación de software, deben estar aprobadas por el Gerente o Director del área y su implementación, debe ser realizada por el Proveedor de Tecnología o el encargado de la Gerencia de Producción, quienes deben mantener los soportes de las autorizaciones.

4.8.5 Normas sobre el registro y seguimiento de eventos y evidencia

1. La organización debe establecer los mecanismos, que permitan probar la ocurrencia de un evento o acción y sus entidades originadoras, para esto se deben contar con logs de auditoría en las bases de datos y en los dispositivos de red y seguridad. Los logs habilitados deben en lo posible permitir Identificar: fecha y hora de la actividad, actividad realizada sobre el aplicativo o sistema, actividad realizada sobre las carpetas y archivos, actividad realizada sobre los datos (Insert, update, delete), usuario que las realizó y dato consultado sobre el aplicativo o sistema, si se trata de una modificación o eliminación de datos en un aplicativo debe quedar el dato anterior y el nuevo, dirección IP desde la que se realizó la acción, también se deben registrar los usuarios que inician sesión en el aplicativo y/o sistema, máquina que se conectó remotamente al equipo entre otros.

2. Las carpetas compartidas donde resida información clasificada como sensible podrán tener habilitada la auditoría de tal forma que se puedan conocer las acciones realizadas sobre la información en ella contenida (Apertura, Borrado, Modificación, etc)

3. Se debe realizar backups de los logs de los sistemas de información y sistemas de monitoreo los cuales deben estar alineados con las políticas de backups (tiempos de retención y frecuencia del backup) definidos por los dueños del activo o los que estén definidos legalmente de acuerdo con el tipo de información. Para datos personales, se deben conservar dos años y para monitoreo, cuando existen eventos especiales, los backups se retendrán por el tiempo definido por el Director Administrativo, el Coordinador de Seguridad o la autoridad que lo requiera.

4. Los registros de acciones realizadas por los administradores y operadores de los sistemas de información, se deben proteger contra alteración y acceso no autorizado.

5. Es responsabilidad del proveedor de tecnología, asegurar que los relojes de todos los sistemas, estén sincronizados, para evitar el no repudio.

4.8.6 Normas respecto a auditoría

1. Se deben realizar auditorías mínimo una vez al año a los sistemas, aplicaciones, redes de la organización y bases de datos que contengan datos personales objeto de tratamiento, que contemplen como mínimo:

    - Actividades relacionadas con los activos de información y ciberactivos críticos.
    - La trazabilidad de las acciones en los sistemas de información.
    - Cumplimiento de normas y requerimientos legales aplicables.
    - Evaluación de controles cibernéticos y de seguridad de la información.
    - Cumplimiento de políticas y procedimientos.
    - Control del correo electrónico, bloqueo de puertos USB, controles de las impresoras, no uso de quemadores u otros dispositivos de almacenamiento.

2. Termovalle, realizará una auditoría extraordinaria siempre que se realicen modificaciones sustanciales en el sistema de información que puedan afectar al cumplimiento de las medidas de seguridad, con el fin de verificar la adaptación, adecuación y eficacia de las mismas.

3. Los responsables de seguridad de las bases de datos automatizadas se encargan de controlar los mecanismos que permiten el registro de acceso, revisar con carácter mensual la información de control registrada y elaborar un informe de las revisiones realizadas y los problemas detectados. Además, deben impedir la manipulación o desactivación de los mecanismos que permiten el registro de acceso.

4. De las auditorías debe quedar un informe de las deficiencias o riesgos encontrados y este debe ser entregado al Coordinador de Riesgos y Cumplimiento.

4.9 SEGURIDAD DE LAS COMUNICACIONES

4.9.1 Normas para la gestión de la seguridad en las redes

1. Los equipos asignados a la operación deben estar en un segmento de red diferente al de toda la compañía utilizando VLAN o dispositivos de red dedicados.

2. Cada mes, se debe realizar monitoreo de conexiones y análisis de tráfico de red para detectar anomalías en el tráfico de red. Este monitoreo debe ser realizado por el proveedor de comunicaciones e informado al proveedor de tecnología. Los casos que generan riesgo a la organización, deben ser gestionados por el proveedor de tecnología e informados al Coordinador de Riesgos y Cumplimiento.

3. Los computadores portátiles y dispositivos móviles que ingresen a la organización, solo podrán ser conectados a la red de invitados.

4. No se debe utilizar ningún punto de red, con equipos diferentes a los asignados a las actividades del proceso.

5. Los cuartos de comunicaciones, deben mantenerse cerrados y con acceso restringido.

4.9.2 Normas para el uso de correo electrónico

Los correos electrónicos, no pueden tener adjuntos que en su totalidad sumen más de 20 Megas.

4.9.3 Normas para el mantenimiento de los navegadores

Cuando se requiera, el proveedor de tecnología, debe realizar una revisión de cada equipo de la compañía, ejecutando el programa de borrado de Cookies, archivos temporales, rastros de passwords guardados, historial, entre otros.

4.10 ADQUISIÓN, DESARROLLO Y MANTENIMIENTO DEL SISTEMA.

1. Todos los requerimientos para la adquisición de software, deben especificar los requisitos respecto a la calidad, funcionalidad y seguridad de la información.

2. Todo software adquirido, debe ser probado respecto a los requisitos solicitados incluyendo los de seguridad de la información y debe contar con soporte del proveedor o fabricante.

3. Los datos para realizar pruebas, deben ser seleccionados y en lo posible enmascarados para proteger su confidencialidad.

4. El proveedor de tecnología y/o el responsable de la Gerencia de Producción, deben garantizar que una vez realizadas las pruebas, los datos proporcionados, sean borrados.

5. Los cambios de versión o migración de sistemas, deben ser aprobados y probados previamente al paso a producción por el dueño del activo.

6. El proveedor de tecnología, es responsable por llevar el control de los cambios en los sistemas.

7. El Director Administrativo y Financiero, deben garantizar que el software adquirido, cuenta con el acuerdo de licenciamiento, condiciones de uso y propiedad intelectual.

8. Los dueños de los activos, debe respetar, proteger y reconocer el derecho a la paternidad de productos y servicios que hayan desarrollado terceros.

4.11 RELACIONES CON LS PROVEEDORES

1. Los terceros que sean vinculados a la organización y que generen riesgo para la seguridad de la información y ciberseguridad, deben firmar una cláusula de confidencialidad, donde se establezcan sus responsabilidades frente a la Seguridad de la Información y su compromiso de no divulgar información interna o externa o la relacionada con sus funciones a través de ningún canal, sin previa autorización.

2. Todos los terceros vinculados con la organización, deben manejar la información a la que tenga acceso y que sea verbal, física o electrónica, de forma íntegra e integral, es decir que se debe adoptar, procesar, entregar o transmitir integralmente y coherentemente, sin modificaciones, ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información.

3. Los terceros, clientes y proveedores, que requieran acceso a la red privada de la organización, deben contar con las medidas de seguridad que aplican internamente, su acceso debe ser restringido a un segmento de red separado del resto de la organización establecido para este fin. En caso que el tercero requiera el acceso a un segmento de red interno, para el desarrollo de una labor específica, se debe contar con la aprobación del Gerente del área y se debe dejar documentado.

4. Los dueños de los contratos, deben garantizar que ante un cambio del alcance del contrato con el tercero, se evalúen los requisitos de seguridad de la información.

5. Termovalle, en cualquier momento durante la relación contractual, puede hacer revisiones de seguridad a los contratistas que apoyan en la empresa y la forma en que ellos protegen su información.

4.12 GESTIÓN DE INCIDENTES CIBERNÉTICOS O DE SEGURIDAD DE LA INFORMACIÓN.

1. Es obligación de todos los empleados que tengan acceso a los activos de información de la organización, incluyendo a las bases de datos que contienen datos personales, reportar los incidentes reales y potenciales de seguridad de la información y cibernéticos. Los incidentes deben ser reportados así:

Ejm: Pérdida de información, acceso no autorizado, denegación del servicio, saboteo de operaciones, interrupción del negocio, daño a la infraestructura y almacenamiento de datos, fuga de información, infección de virus, ataques cibernéticos e infidelidad interna, entre otros.

Quién identifique el incidente, debe reportar a:

- Proveedor de Tecnología para temas administrativos
- Líder de mantenimiento para temas de la planta de producción
- Responsable de seguridad, para temas relacionados con datos personales

Nota: Si el incidente es ocasionado por un tercero, el empleado responsable del tercero, es quién debe realizar el reporte.

Quién recibe el reporte, debe realizar las acciones inmediatas para solucionarlo

Quién recibe la notificación del incidente, debe Reportar al Coordinador de Riesgos y Cumplimiento a través del formato de reporte de eventos de riesgo.

2. Los eventos que se deban informar a las autoridades, serán evaluados por el Coordinador de Protección Integral, por el Jefe Legal y/o por el Coordinador de Riesgos, estos pueden ser también evaluados y/o aprobados por el Comité de Riesgos. El reporte a las autoridades solo puede ser realizado por el Coordinador de Protección Integral o el Jefe Legal.

3. Dentro del marco de atención de incidentes deben existir planes específicos de respuesta.

4. El Coordinador de Riesgos y Cumplimiento, debe velar porque los incidentes cuenten con su correspondiente investigación por parte de personal calificado, para determinar la causa raíz y de acuerdo con esta, se deben realizar planes de tratamiento para evitar que vuelvan a suceder. La Coordinación de Riesgos y Cumplimiento, debe hacer seguimiento a su cumplimiento y eficacia.

5. Se deben establecer procedimientos para la identificación, recolección, adquisición y preservación de la evidencia relacionada con el incidente de seguridad de la información.

6. El Coordinador de Riesgos y Cumplimiento, debe documentar los incidentes cibernéticos y de seguridad de la información y todo lo relacionado con ellos, en una base de datos, la cual servirá como fuente de análisis para retroalimentar la matriz de riesgos y reducir la posibilidad o el impacto de futuros incidentes. Estos incidentes, deben ser informados al Comité de Riesgos de forma trimestral

4.13 CONTINUIDAD DEL NEGOCIO

4.13.1 Normas respecto a la continuidad del negocio

1. El Coordinador de Riesgos y Cumplimiento junto con los líderes de proceso, establecerán las situaciones que pueden generar eventos de continuidad del negocio. Estos deben ser revisados y aprobados por el Comité de Riesgos.

2. El Coordinador de riesgos realizará junto con los líderes de proceso y el Jefe de Recursos Humanos, realizaran el análisis de impacto al negocio (BIA), con el fin de establecer los niveles de disponibilidad de los servicios e información que manejan de acuerdo con requisitos legales, niveles de servicio requeridos por las partes interesadas o riesgos evaluados.

3. De acuerdo con el análisis de impacto al negocio (BIA), la organización debe definir los planes de recuperación y de respaldo de la información de acuerdo a las necesidades de disponibilidad del negocio.

4. Los planes de recuperación deben incluir los procesos y procedimientos para el respaldo y almacenamiento de la información necesaria para la recuperación efectiva de los ciber activos críticos. El respaldo debe incluir entre otros los equipos, componentes electrónicos para reposición, la documentación de parámetros de configuración, software y el respaldo de datos.

5. Implementar un mecanismo para la obtención de imágenes de los sistemas operativos y las configuraciones de los Servidores con el fin de facilitar la

recuperación de los mismos de manera más ágil que teniendo que volver configurar en caso de desastre.

6. Los planes de recuperación deben probarse mínimo una vez al año. Una prueba o simulacro del plan de recuperación puede comprender desde una prueba de escritorio a un ejercicio operativo completo que simule un incidente real. De este, debe quedar evidencia documentada de la realización de las mismas. Los resultados serán informados al Comité de Riesgos, por parte del Coordinador de Riesgos y Cumplimiento.

7. La información esencial de recuperación que se almacene en medios de respaldo debe ser probada mínimo una vez al año para asegurar que la información sea integra y esté disponible.

8. Los planes de recuperación deben actualizarse para reflejar los cambios, planes de mejoramiento y lecciones aprendidas de las pruebas o simulacros o de las recuperaciones ante incidentes reales.

4.13.2 Normas sobre copias de respaldo

1. El proveedor de tecnología es responsable de realizar copias de respaldo de la información, software e imágenes de los sistemas de la organización.
2. Las copias de respaldo de la información, se deben hacer diariamente.
3. El proveedor de tecnología, debe poner a prueba cada seis meses (6), la restauración de las copias de respaldo, para probar su integridad y disponibilidad en el momento que se requiera. De estas pruebas debe dejar evidencia y los resultados deben ser informados a la Dirección Financiera y Administrativa y a la Coordinación de Riesgos y Cumplimiento.
4. El proveedor de tecnología, debe garantizar que se almacene una copia de la información de los servidores diaria en un medio externo ubicado en el mismo lugar que el servidor y una segunda copia en la nube.
5. La información de la operación, se debe realizar backup cada 6 meses o cada vez que exista un cambio significativo.
6. El tiempo de retención de las copias de respaldo de la información, debe ser definido por el dueño del activo de acuerdo a los requisitos normativos o políticas internas, estimando el RPO de los datos y considerando la capacidad de reconstrucción de los mismos.

4.13.3 Normas respecto a redundancias

1. La Gerencia de Producción y el proveedor de Tecnología, deben establecer los requerimientos de redundancia de los sistemas o plataformas tecnológicas de la organización, de acuerdo a su criticidad.

2. El canal de acceso a internet, debe contar con un sistema redundante, para los casos que decida la Dirección Financiera y Administrativa.

4.14 CUMPLIMIENTO

1. La Jefatura de Asuntos legales, debe identificar, documentar y mantener actualizados los requisitos estatutarios, reglamentarios y contractuales relacionados con la seguridad cibernética y seguridad de la información.

2. La organización se compromete a proteger contra un uso no autorizado los derechos de autor, patentes, marcas, diseños, invenciones tanto de Termovalle como de los terceros.

3. Toda información, diseño de procesos, invenciones, mejoras u otros que origine cualquier empleado como parte de sus funciones, es derecho exclusivo de Termovalle.

4. El proveedor de tecnología, debe establecer controles para garantizar que todo el hardware y software de la organización, cuente con su correspondiente licencia.

4.15 PROTECCIÓN DE DATOS PERSONALES

1. La política de protección de datos personales y del tratamiento de los mismos, será aprobada por la Jefatura Legal y la Gerente General.

2. La política de Protección de datos personales, debe estar publicada en la página web de la organización.

3. La Coordinación de Riesgos y Cumplimiento, debe establecer un plan de comunicaciones para que la política sea conocida por el personal de Termovalle.

4. El reporte de los nombres de las bases de datos y de las políticas a la Superintendencia de Industria y Comercio (SIC), es responsabilidad de la Jefatura Legal.